UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/061,415	02/01/2002	Davide Libenzi	002.0259.01	9282

28875 7590 06/16/2006

Zilka-Kotab, PC
P.O. BOX 721120
SAN JOSE, CA 95172-1120

EXAMINER	
HENNING, MATTHEW T	
ART UNIT	**PAPER NUMBER**
2131	

DATE MAILED: 06/16/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 10/061,415
Filing Date: February 01, 2002
Appellant(s): LIBENZI ET AL.

Kevin J. Zilka
Reg. No. 41,429
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed April 03, 2006 appealing from the Office action mailed November 09, 2005.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

No amendment after final has been filed.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

Appellant's brief presents arguments relating to the objection to the specification under 37 CFR 1.75(d)(1) as failing to provide proper antecedent basis for the claimed subject matter. This issue relates to petitionable subject matter under 37 CFR 1.181 and not to appealable subject matter. See MPEP § 1002 and § 1201.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

6,381,242	Maher III et al.	4-2002
6,275,937	Hailpern et al.	8-2001

6,785,732	Bates et al.	8-2004
6,684,329	Epstein et al.	1-2004

Stevens, W.R. "TCP/IP Illustrated, Volume 1", 1994 Addison Wesley, pp. 6-11 and Inside Cover

Microsoft Press Computer Dictionary Third Edition, 1997, Microsoft Corporation, pp. 392

The American Heritage College Dictionary Fourth Edition, 2002, Houghton Mifflin Company, pp. 368 and 1018

OSI Model, Wikipedia, http://en.wikipedia.org/wiki/OSI_model, accessed June 1, 2006

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claim Rejections - 35 USC § 112

The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

Claims 32-38, 40-47, and 49-54 rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claims contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventors, at the time the application was filed, had possession of the claimed invention. Claims 32 and 41 recite that "each of a plurality of protocol-specific modules process each reassembled datagram based on an upper protocol layer employed by the reassembled datagram". Although there is support for multiple sub-modules in the scanner, there is no

support for a plurality of separate modules which each process each datagram. As such, the ordinary person skilled in the art would not be able to determine whether the applicants were in possession of the claimed invention at the time of filing. Therefore, claims 32 and 41 are rejected for failing to meet the written description requirement of 35 USC 112 1st paragraph. Claims 33-38, 40, 42-47, and 49-54 are rejected by virtue of their dependency to claims 32 and 41.

Claims 53-54 recite "a plurality of protocol-specific scanning sub-modules, each protocol specific scanning sub-module designated for scanning network protocol packets of a particular protocol". Although there is support for the protocol-specific scanning sub-modules, there is no support that they actually scan the packets. Instead, the specification provides support that they simply are used to retrieve the packets and provide them to the scanner. As such, the ordinary person skilled in the art would be unable to determine whether the applicants were in possession of the claimed invention at the time of filing. Therefore, claims 53-54 are rejected for failing to meet the written description requirement of 35 USC 112 1st paragraph.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an

application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1-10, 13-14, 16-25, 28-29, 31 and 55 are rejected under 35 U.S.C. 102(e) as being anticipated by Maher, III et al. (US Patent Number 6,381,242) hereinafter referred to as Maher.

Regarding claim 1, Maher disclosed a system for providing passive screening of transient messages in a distributed computing environment (See Maher Abstract), comprising: a network interface passively monitoring a transient packet stream at a network boundary (See Maher Column 5 lines 46-54 and Col. 7 Lines 13-15) comprising receiving incoming datagrams structured in compliance with a network protocol layer (See Maher Col. 5 Lines 46-54 and Col. 3 Lines 54-67 wherein it was inherent that the packets were compliant with a network layer in order for them to be transmitted through the network); a packet receiver reassembling one or more of the incoming datagrams into a segment structured in compliance with a transport protocol layer (See Maher Col. 5 Line 60 - Col. 6 Line 7); an antivirus scanner scanning contents of the reassembled segment for a presence of at least one of a computer virus and malware to identify infected message contents (See Maher Col. 10 Lines 42-46), and a protocol-specific module processing each reassembled datagram based on the transport layer protocol employed by the reassembled datagram (See Maher Col. 7 Lines 18-30).

Regarding claim 16, Maher disclosed a method for passive screening of transient messages in a distributed computing environment (See Maher Abstract), comprising: passively monitoring a transient packet stream at a network boundary (See Maher Column 5 lines 46-54 and Col. 7 Lines 13-15) comprising receiving incoming datagrams structured in compliance with a network protocol layer (See Maher Col. 5 Lines 46-54 and Col. 3 Lines 54-67 wherein it was

inherent that the packets were compliant with a network layer in order for them to be transmitted through the network); reassembling one or more of the incoming datagrams into a segment structured in compliance with a transport protocol layer (See Maher Col. 5 Line 60 - Col. 6 Line 7); scanning contents of the reassembled segment for a presence of at least one of a computer virus and malware to identify infected message contents (See Maher Col. 10 Lines 42-46), and processing each reassembled datagram based on the transport layer protocol employed by the reassembled datagram (See Maher Col. 7 Lines 18-30).

Regarding claims 2 and 17, Maher disclosed an incoming queue staging each incoming datagram intermediate to reassembly (See Maher Col. 8 Lines 42-51).

Regarding claims 3 and 18, Maher disclosed a network protocol-specific decoder decoding the reassembled segment prior to scanning (See Maher Col. 5 Line 65 – Col. 6 Line 1).

Regarding claims 4 and 19, Maher disclosed that the antivirus scanner terminates the transient packet stream if the reassembled segment is not infected with at least one of a computer virus and malware (See Maher Col. 7 Lines 30-33).

Regarding claims 5 and 20, Maher disclosed that the antivirus scanner takes an action if the reassembled segment is infected with at least one of a computer virus and malware (See Maher Col. 10 Lines 42-46).

Regarding claims 6 and 21, Maher disclosed that the action comprises at least one of logging an infection; generating a warning; spoofing a valid datagram in place of the infected datagram (See Maher Col. 10 Lines 42-46); and acquiescing to the infection.

Regarding claims 7 and 22, Maher disclosed a protocol-specific queue staging each reassembled segment with other reassembled segments sharing the same transport protocol layer (See Maher Col. 7 Lines 18-30).

Regarding claims 8 and 23, Maher disclosed an information record storing information dependent on the same transport protocol layer with the staged reassembled segment (See Maher Col. 6 Lines 12-22).

Regarding claims 9 and 24, Maher disclosed a contents record storing the contents with the staged reassembled segment (See Maher Col. 6 Lines 12-19).

Regarding claims 10 and 25, Maher disclosed that the information comprises at least one of a source address, source port number, destination address, destination port number, URL, file name, user name, sender identification, recipient identification, and subject (See Maher Col. 6 Lines 20-22).

Regarding claims 13 and 28, Maher disclosed an event correlator analyzing the transient packet stream for events indicative of a network service attack (See Maher Col. 7 Lines 35-50).

Regarding claims 14 and 29, Maher disclosed a data repository maintaining each event (See Maher Col. 7 Lines 40-48).

Regarding claim 55, Maher disclosed that the incoming datagrams include IP datagrams that are reassembled into TCP segments (See Maher Col. 6 Lines 4-7 and Col. 7 Paragraph 3 wherein it was inherent that the PDUs of the email data was processed to TCP segments in order to get the payload of the data for scanning.)

Claim 31 is rejected for the same reasons as claims 16-25, and 28-29 and further because Maher disclosed processors executing the described functions (See Maher Col. 11 lines 34-37).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 32-35, 38, 41-44, 47, and 50-52 are rejected under 35 U.S.C. 103(a) as being unpatentable over Maher, as evidenced by Stevens (TCP/IP Illustrated Vol. 1).

Regarding claim 32, Maher disclosed a system for passively detecting computer viruses and malware and denial of service-type network attacks in a distributed computing environment, comprising: a network interface receiving copies of datagrams transiting a boundary of a network domain into an incoming packet queue, each datagram being copied fro a packet stream (See Maher Col. 5 Paragraph 4 Fast Access Bus); a packet receiver reassembling one or more of the incoming datagrams from the incoming packet queue into network protocol packets, each staged in a reassembled packet queue (See Maher Col. 5 Line 60 - Col. 6 Line 14); an antivirus scanner scanning each network protocol packet from the reassembled packet queue to ascertain an infection of at least one of a computer virus and malware (See Maher Col. 10 Lines 42-46), and an event correlator evaluating events identified from the datagrams in the packet stream to

detect a denial of service-type network attack on the network domain (See Maher Col. Col. 7 Lines 35-50), and disclosed determining the type of data the packets contained (See Maher Col. 7 Paragraph 3) as well as scanning the payload of the packets (See Maher Col. 10 Lines 42-46), however Maher failed to disclose how the data type of the packet was ascertained or how the payload was retrieved.

It was well known that in the Internet Protocol there are multiple layers and that each layer contains different modules, such as the TCP module and the UDP module of the transport layer. It was also well known that in order to get to the data in the application layer packet, such as the payload and the packet type, the transport layer module must process the transport layer packet to reveal the application layer packet. This is evidenced by Richards Pages 6-11.

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ what was well known in the art of networking and TCP/IP in order to gain access to the data in the packets for scanning and queuing. This would have been obvious because the ordinary person skilled in the art would have been motivated to use what was well known in the art.

Regarding claim 41, Maher disclosed a method for passively detecting computer viruses and malware and denial of service-type network attacks in a distributed computing environment, comprising: receiving copies of datagrams transiting a boundary of a network domain into an incoming packet queue, each datagram being copied fro a packet stream (See Maher Col. 5 Paragraph 4 Fast Access Bus); reassembling one or more of the incoming datagrams from the incoming packet queue into network protocol packets, each staged in a reassembled packet queue (See Maher Col. 5 Line 60 - Col. 6 Line 14); scanning each network protocol packet from the

reassembled packet queue to ascertain an infection of at least one of a computer virus and malware (See Maher Col. 10 Lines 42-46), and evaluating events identified from the datagrams in the packet stream to detect a denial of service-type network attack on the network domain (See Maher Col. Col. 7 Lines 35-50), and disclosed determining the type of data the packets contained (See Maher Col. 7 Paragraph 3) as well as scanning the payload of the packets (See Maher Col. 10 Lines 42-46), however Maher failed to disclose how the data type of the packet was ascertained or how the payload was retrieved.

It was well known that in the Internet Protocol there are multiple layers and that each layer contains different modules, such as the TCP module and the UDP module of the transport layer. It was also well known that in order to get to the data in the application layer packet, such as the payload and the packet type, the transport layer module must process the transport layer packet to reveal the application layer packet. This is evidenced by Richards Pages 6-11.

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ what was well known in the art of networking and TCP/IP in order to gain access to the data in the packets for scanning and queuing. This would have been obvious because the ordinary person skilled in the art would have been motivated to use what was well known in the art.

Regarding claims 33 and 42, Maher disclosed a parser parsing each reassembled datagram into network protocol-specific information and packet content (See Maher Col. 5 Line 65 – Col. 6 Line 19).

Regarding claims 34 and 43, Maher disclosed extracting the header information from the packets (See the rejection of claim 33 above), but failed to disclose specifically what information

was contained in the headers. It was well known in the art at the time of invention that the headers of HTTP messages contained a source address and port number, a destination address and port number, and a URL, the headers of an FTP message contained the filename and username, and the headers for the SMTP contained the sender identifier, receiver identifier, and subject. As such, it would have been obvious to the ordinary person skilled in the art at the time of invention to employ what was well known by extracting the header information from the headers of the packets. This would have been obvious because the ordinary person would have been motivated to extract what was known to be contained in the header.

Regarding claim 35 and 44, Maher disclosed a decoder decoding the packet content prior to performing the operation of scanning (See Maher Col. 5 Line 65 – Col. 6 Line 1 and Col. 2 Lines 9-12).

Regarding claim 38 and 47, Maher disclosed a spoof module sending a spoofed network protocol packet responsive to an occurrence of at least one of the infection and the network attack (See Maher Col. 10 Lines 42-46).

Claim 50 is rejected for the same reasons as claims 32-33, 35, 38, 41-42, 44, and 47 and further because Maher disclosed processors executing the described functions (See Maher Col. 11 lines 34-37).

Regarding claim 51, Maher disclosed that the packets comprised general "web surfing" traffic, email traffic, and VoIP traffic (See Maher Col. 7 Paragraph 3), but failed to specifically disclose the specific protocols used for each. It was well known at the time invention that general web surfing traffic utilized HTTP, and that email traffic utilized SMTP (Simple Mail Transport Protocol) and POP3. Therefore, it would have been obvious to the ordinary person

skilled in the art at the time of invention to employ what was well known in the art by using the HTTP, SMTP, and POP3 protocols. This would have been obvious because the ordinary person skilled in the art would have been motivated to use the protocols that were standard in the art.

Regarding claim 52, Maher disclosed that only datagrams compliant with IP protocol are reassembled (See Maher entire reference especially the last paragraph of Col. 3, wherein only IP type traffic was disclosed).

Claims 15, 30, 40, and 49 are rejected under 35 U.S.C. 103(a) as being unpatentable over Maher as applied to claims 1, 16, 32, and 41 above, and further in view of Hailpern et al. (US Patent Number 6,275,937) hereinafter referred to as Hailpern.

Maher disclosed a system for scanning IP network packets for viruses (See the rejection of claim 1 above and Col. 3 Lines 54-67), but failed to disclose that all the incoming messages were SMTP compliant, and therefore TCP compliant.

Hailpern teaches that virus scanning should be set up for each network protocol proxy, including E-mail, in order to scan for viruses (See Hailpern Col. 4 Lines 1-13).

It would have been obvious to the ordinary person skilled in the art to employ the teachings of Hailpern in the virus scanning system of Maher by modifying mail servers to contain the scanning system of Maher. This would have been obvious because the ordinary person skilled in the art would have been motivated to enable the proxies to be able to scan the types of communications they already process and therefore reduce network traffic and delay. Further, SMTP mail servers were well known in the art at the time of invention, and it would have been obvious to utilize the scanning system of Maher in an SMTP mail server. This would

have been obvious because the ordinary person skilled in the art would have been motivated to protect SMTP mail servers from viruses.

Claims 36-37 and 45-46 are rejected under 35 U.S.C. 103(a) as being unpatentable over Maher as applied to claims 32 and 41 above, and further in view of Bates et al. (US Patent Number 6,785,732) hereinafter referred to as Bates.

Maher disclosed detecting viruses in network packets (See the rejection of claim 38 above), but failed to disclose logging the detection or generating a warning.

Bates teaches that upon detecting a virus, the detection should be logged and a warning should be generated (See Bates Col. 12 Lines 41-48 and Col. 10 Lines 2-8).

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Bates in the packet scanning system of Maher by logging virus detections and generating warnings in the event of virus detection. This would have been obvious because the ordinary person skilled in the art would have been motivated to enable the server to analyze the virus activity and to alert the sender of the virus of the virus.

Claims 53-54 are rejected under 35 U.S.C. 103(a) as being unpatentable over Maher as applied to claim 32 above, and further in view of Epstein et al. (US Patent Number 6,684,329) hereinafter referred to as Epstein.

Maher disclosed scanning packets for viruses (See Maher Col. 6 Line 59 – Col. 7 Line 6), but failed to disclose sub-modules which each scan one of HTTP, FTP, SMTP, and NNTP packets.

Epstein teaches that in a firewall which scans for viruses, proxy sub-modules should be provided in the firewall for each of HTTP, FTP, SMTP, and NNTP protocol packets (See Epstein Col. 1 Lines 27-53 and Col. 3 Lines 8-21).

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Epstein in the virus scanning of Maher by providing protocol specific proxy servers in the firewall to scan each of HTTP, SMTP, FTP, and NNTP packets. This would have been obvious because the ordinary person skilled in the art would have been motivated to provide the network administrator with greater control over the traffic which traversed the content processor.

(10) Response to Argument

The appellant has presented seven (7) different issues.

Issue #1

The appellant argues against the objection to the specification as failing to provide proper antecedent basis for the claimed subject matter. However, as pointed out above in section 6, this issue relates to petitionable subject matter under 37 CFR 1.181 and not to appealable subject matter. See MPEP § 1002 and § 1201. As such, the objection has not been addressed further. However, a related rejection under 35 USC 112 1st Paragraph has been discussed below in relation to Issue #2.

Issue #2

The appellant argues with regards to claim 32, that the recitation "**each** of a plurality of protocol-specific modules **process each** reassembled datagram based on an upper protocol layer employed by the reassembled datagram" does not require that "each separate module processes each datagram". The examiner disagrees with this argument and points out that the claim language clearly states that each of a plurality of modules process each datagram. As such, the examiner has read the claim as it is written. The appellant further argues that this limitation is supported by the specification on Page 7 Line 29 – Page 8 Line 5.

> *The antivirus scanner 32 includes a plurality of protocol-specific scanning submodules 35-38, including submodules for the Hypertext Protocol (HTTP), File Transfer Protocol (FTP), Simple Mail Transport Protocol (SMTP), and Network News Transport Protocol (NNTP), although other upper layer network protocols could also be implemented, as would be recognized by one skilled in the art.*
>
> *Through each protocol-specific submodule 35-38, the antivirus scanner 32 retrieves each re-assembled packet from the appropriate protocol-specific queue 41 for scanning using standard antivirus techniques, as are known in the art.*

These two paragraphs simply state that the antivirus scanner retrieves the re-assembled packets through the protocol specific submodules. This does not support the limitation that "**each** of a plurality of protocol-specific modules **process each** reassembled datagram based on an upper protocol layer employed by the reassembled datagram" and as such, the claim fails to meet the written description requirement of 35 USC 112 1st Paragraph.

The appellant argues with respect to claims 53-54 that the above cited section of the specification, Page 7 Line 29 – Page 8 Line 5, supports the limitation of "a plurality of protocol-specific scanning submodules, each protocol specific scanning sub-module **designated for scanning** network protocol packets of a particular protocol" where the cited section says "[t]hrough each protocol-specific submodule...scanning using standard antivirus techniques". However, the appellant only highlighted the submodule and scanning in the citation. This is misleading as the actual citation states that "[t]hrough each protocol specific submodule 35-38, the antivirus scanner **retrieves** each re-assembled packet...for scanning using standard antivirus techniques". It is readily seen that in fact it is the antivirus scanner that performs the scanning, and not the submodules, as the appellant contends.

Issue #3

The appellant argues that because the "physical interface" 102 of Maher III et al. (hereinafter referred to as Maher), "frames the data, and then formats the data for placement on the fast path bus 126" that the "physical interface is not "passive". The examiner first points out that the specification of the instant application is silent regarding any sort of definition of "passive". As such, the examiner points to *The American Heritage College Dictionary*'s definition of "passive" on page 1018, which recites "receiving or subjected to an action without responding or initiating an action in return." In other words, not reactive. In this case, although the "physical interface" does frame and format the data that it receives, the "physical interface" does not "react" to the data that is received, but instead acts in the same manner on all data it

receives. As such, the "physical interface" is "passive" because it does not respond to the data that is received.

The appellant further argues that the 'fast-path data bus 126" of Maher is also not passive because it "feeds" data to the scanning processor, and further is not a "network interface". The examiner points out that although Maher did not specifically refer to the "fast-path data bus" as a "network interface", it is in fact a network interface for the scanning processor 140, as it is the interface to the scanning processor which provides the scanning processor with network data. Further, by similar reasoning presented above, the fast-path data bus is "passive". Maher does not disclose the fast-path data bus reacting to the data, but rather the fast-path data bus simply passes on the received data. This is analogous to an electric wire, which when a signal is applied to one end, the signal is passed through the wire. Clearly, an electric wire is "passive", as is the "fast-path data bus".

The appellant argues that Maher does not reassemble the incoming datagrams in compliance with "a transport layer protocol". The examiner points out that this is not what is recited in the claim, but instead the claim recites that the datagrams be in compliance with "a transport protocol layer". Maher disclosed in Col. 6 Lines 4-7, that the header preprocessor could assemble ATM cells into complete data packets (PDUs). The OSI, or Open Systems Interconnection Reference Model, is a seven layer description of the network transport protocols. These layers include 1. Physical Layer, 2. Data Link Layer, 3. Network Layer, 4. Transport Layer, 5. Session Layer, 6. Presentation Layer, and 7. Application Layer. (Please See the Wikipedia description of OSI for a more detailed description of the OSI model.) Maher disclosed the use of ATM, as well as IP (See a specific example at Col. 5 Line 58 – Col. 6 Line

7). ATM is a data link layer protocol, and IP is a network layer protocol in the OSI model. As such, because the ATM cells of Maher are assembled into complete data packets, the data packets were in compliance with the Data Link Layer. Because the claim language only requires that the datagram be compliant with a layer, Maher meets this limitation by having complete ATM data packets. Further, Maher disclosed stripping the packets of the ATM header information, as seen is Col. 6 Lines 4-7. This stripping of information is commonly known as demultiplexing, and when the header information is stripped from a data link layer packet, a network layer (or IP) datagram is left. (For information regarding packet encapsulation please see Pages 6-11 of *TCP/IP Illustrated Volume 1.*) Therefore, not only does Maher disclose creating datagrams in compliance with the data link layer, Maher also disclosed creating datagrams in compliance with the network layer. As such, Maher meets the limitation of the claim.

The appellant argues that Maher did not disclose a "protocol-specific module processing each reassembled datagram based on the transport protocol layer employed by the reassembled packet" because the QoS processor is not protocol-specific. The points out that the QoS "protocol-specific" because it processes data based on the "protocol" of the data. This is seen in Col. 7 Paragraph 3, wherein Maher disclosed that QoS processor assigns data packets to the internal service quality queues based on the data packet type.

> *This allows QoS processor to assign the necessary bandwidth to traffic flows such as VoIP, video and other flows with high quality and reliability requirements while assigning remaining bandwidth to traffic flows with low quality requirements such as email and general web surfing to low priority queues.*

Furthermore, the appellant argues that data packets are not assigned to a QoS queue based on the application type of the packet. The examiner points out that Maher disclosed that the email packets were located in a low priority queue, and that VoIP packets were located in a high priority queue, as can be seen in the above cited section (Col. 7 Lines 24-30). If the packets were not assigned to the queues based on the application type, how would all the email packets be located in the low priority queue, and the VoIP data be located in the high priority queue? Maher did in fact disclose queuing the packets based on the application type.

The appellant further argues that the application type is not related to a transport protocol layer. The examiner points out that the application type is most certainly associated with the application layer of the OSI model.

Further still, Maher, in Col. 6 Lines 8-26, disclosed the header pre-processor scanning the headers of the packet for certain information including source address, destination address, source port, destination port, and protocol. It is common knowledge that in the OSI model and TCP/IP, that each layer of the model applies its own header to a packet during encapsulation, and each layer strips its respective header from the packet during demultiplexing (See TCP/IP pages 6-11 for a more detailed explanation of this process). It is also common knowledge that the IP header (network layer header) contains the source address and destination address, while the TCP header (transport layer header) contains the source and destination ports. As such, in order to have retrieved this information from the headers, processing based on the header types must have been performed. Further, the processing must have been based on the transport protocol layer that the header was associated with, because knowledge of where the information was

located in the header is required in order to locate the information. As such, the header pre-processor processes based on the specific protocol layers, and is therefore also protocol-specific.

Even further still, the examiner notes that on Page 13 of the appeal brief in the third paragraph Lines 2-6, the appellant admits that Maher meets the limitation of the claim.

The appellant further argues with respect to dependant claim 3, that Maher did not disclose a network protocol-specific decoder decoding the reassembled segment prior to scanning, because the elements pointed to by the examiner accept all data packets and not just one type of data packet. The examiner points out that the claim language does not require that the network protocol-specific decoder only receive one type of packet. The examiner has interpreted "network protocol-specific decoder" to mean a decoder that decodes based on network protocols. As the specification of the instant application appears to be silent regarding this decoder, or decoding the examiner has utilized *the American Heritage College Dictionary*'s definition of decode on page 368, which reads "to extract the underlying meaning from". As previously pointed out, the header pre-processor strips the ATM header off of the ATM cell creating an IP datagram, which falls with in the scope of decoding, as the IP datagram is extracted from the ATM cell. In order to have done this, the header pre-processor must have processed the ATM cell according to the ATM protocol by recognizing which bits were header bits and which were payload bits. As such, the header pre-processor met the limitations of a network protocol-specific decoder. Further, as previously pointed out, the header pre-processor creates a session id from the contents of the headers of the packets (See Maher Col. 6 Paragraph 3). Again, this required that the header pre-processor processed the packets based on the specific

protocol of the packet. This is because the headers of different protocols are not necessarily the same (See TCP/IP Illustrated Inside Cover). As such, the header pre-processor extracted the underlying meaning of the header bits, and did so based on the particular protocol type of the header. As such, the header pre-processor further meets the limitation of "a network protocol-specific decoder".

The appellant argues, regarding claim 4, that Maher does not disclose "wherein the antivirus scanner terminates the transient packet stream of the reassembled segment is not infected with at least one of a computer virus and malware" because Maher does not disclose termination depending on whether there is a match. The examiner points out that the claim language does not require termination depending on whether there is a match, or that in all cases in which a match is not made, termination occurs, or even that in only cases when a match is not made, termination occurs. Rather, the limitation requires that in at least one case when a match is not made, termination occurs. Maher disclosed that packets which are not infected (there was no match during scanning) are placed in the QoS queues, and if there is not enough bandwidth to process all the packets, the packets are selectively terminated, as can be seen in Maher Col. 7 Lines 7-33. As such, Maher meets the limitation of the claim. Further still, Maher disclosed that while the scanner is scanning a traffic flow, the scanner determines the state of the traffic flow. In an intermediate state, the scanner requests more data to continue scanning, as can be seen in Maher Col. 9 Lines 58-65, and that once it has been determined that there is or isn't a match, scanning is complete, no more data requests are performed and the traffic flow to the

scanner is stopped, as can be seen in Col. 9 Line 65 – Col. 10 Line 5. As such, Maher meets the limitations of the claim.

The appellant argues, with respect to claim 6, that Maher did not disclose all of "logging an infection, generating a warning, spoofing a valid datagram in place of the infected datagram, and acquiescing to the infection". However, the claim recites that only "at least one of" these is required, and Maher disclosed altering the bits of an infected attachment, as seen in Col. 10 Lines 42-46. The specification of the instant application on page 12 Lines 29-31 only recites that sending a valid packet is "spoofing". Maher disclosed sending the email after altering the bits of the infected message in order to render it harmless. In turn, this would send valid, and different, datagrams in place of the originally infected datagrams. This meets the requirements of the appellant's usage of the term "spoof".

The appellant argues that because email may employ various protocols, including IMAP, POP3, SMTP, and HTTP, the IP datagrams would not necessarily be required to be assembled into TCP segments. As discussed above with regards to the OSI layers, in order to get from the Data Link Layer (ATM) to the Application layer (where the appellant's list of email protocols, IMAP, POP3, SMTP, and HTTP, are located), the system had to strip off the ATM header to arrive at the Network layer, then strip off the Network layer header to arrive at the Transport layer (where TCP is located), then strip off the Transport layer header to arrive at the Session layer, then strip off the Session layer header to arrive at the Presentation layer, and finally strip off the Presentation layer header to arrive at the Application layer (this is shown in very clearly

in Fig. 1.7 on Page 10 of TCP/IP illustrated). Further, it is known that IP based email protocols, including the four listed by the appellant, are also TCP based email protocols. As such, to get to the application layer, TCP segments must have been created, and therefore, Maher meets this limitation.

Issue #4

The appellant argues, regarding claim 32, that Maher does not disclose receiving copies of datagrams, but instead actual datagrams. The examiner points out that in computing, and particularly in networking, when data is "transmitted" from a sender to a receiver, the receiving end does not receive a physical object, but instead receives signals which are interpreted by the receiver to recreate the data. As such, when the sender transmits a message, which is simply a collection of binary bits, each signal that is transmitted across the network is an electrical representation of each bit in the message that is being transmitted. Similarly, when a sender transmits a "datagram", signals which represent the collection of bits of the datagram are carried across the network, and the recipient uses these signals to recreate the datagram. As such, the recreated datagram is a copied datagram. Therefore, Maher meets the limitation of receiving copied datagrams.

The appellant argues that Maher did not specifically teach reassembling one or more datagrams into network protocol packets. The examiner again points out that Maher disclosed reassembling one or more ATM cells into complete data packets including removal of the ATM header in Col. 6 Lines 4-7 and as explained above, this creates a network layer packet. Please

see TCP/IP Illustrated Pages 6-11 and the above remarks regarding encapsulation and demultiplexing for a more in depth explanation of the OSI model.

The appellant further argues that Maher did not disclose "a reassembled packet queue". Maher clearly disclosed placing the reassembled packets into a packet storage memory while they are processed by the content processor, which scans the packets, as can be seen in Col. 6 Lines 4-16. The *Microsoft Computer Dictionary Third Edition* defines a "queue" as "a multi-element data structure from which (by strict definition) elements can be removed only in the same order in which they were inserted", and further goes on to say that "[t]here also several types of queues in which removal is based on factors other than order of insertion". Since the appellant's specification is silent as to the definition of a queue, and the claim does not require the queue to be a first in first out queue, the examiner has not read this limitation into the claim. As such, a memory, which is a multi-element data structure, which stores the reassembled packets until they are scanned, falls within the scope of "a reassembled packet queue".

The appellant argues that Maher did not disclose plural "protocol-specific modules" for processing the reassembled datagram based on an upper layer protocol. Maher did disclose that the packets are placed in a priority queues based on the type of application, as previously discussed, (See Maher Col. 7 Lines 18-30). The only processing performed by the "protocol-specific modules" of the present application is getting data from a queue and sending it to be scanned. The queues receive data of specific protocols and send them out onto the network, as is seen in Col. 7 Paragraph 3. As such, the queues meet this limitation in the same manner that the

present invention meets the limitation. Furthermore, as discussed above, Maher uses the OSI model and also scans the content of the packets. Therefore, as discussed previously, in order to get to the contents of the packet, it had to be demultiplexed which required each layer (module) to process the packet and remove its header before passing the packet up the OSI stack. As such, each layer of the OSI stack is a protocol-specific module which processes each packet based on the protocol used by the packet. As such, Maher did disclose multiple protocol-specific modules processing the reassembled packets based on an upper protocol layer.

The examiner notes that in regards to claim 32, the appellant argues that Maher did not disclose processing each reassembled datagram based on the transport protocol layer employed by the reassembled datagram. However, the examiner has not addressed this particular argument in view of the fact that this limitation is not recited in claim 32.

The appellant argues, in regards to claim 52, that Maher did not disclose that only datagrams compliant with IP protocol are reassembled. The examiner agrees that Maher did not specifically state that only IP protocol datagrams are reassembled, but Maher did disclose that this was for use with the IP protocol, as can be seen in Maher Col. 3 Last Paragraph, and nowhere in Maher is there any suggestion of using any non-IP network protocol. As such, Maher only disclosed reassembling IP datagrams and did not disclose reassembling any other types of network layer datagrams.

Regarding Issues #5, #6, and #7, the examiner notes that no new arguments have been presented. However, the examiner notes that Bates et al., which was relied upon for claims 36-37 and 45-46 teach that detection of a virus should be logged and a warning should be generated.

To summarize, the examiner has addressed the appellant's arguments:

As per Issue #1, the examiner has shown that this is not an appealable issue.

As per Issue #2, the examiner has shown that the specification does not meet the written description requirement for claims 32-38, 40-47, and 49-54.

As per Issue #3, the examiner has shown that Maher did disclose, specifically or inherently, a passive network interface; reassembling datagrams in compliance with a transport protocol layer; a protocol specific module processing each reassembled datagram based on the transport protocol layer of the packet; queuing packets based on the protocol of the packets; a network protocol specific decoder; terminating a stream if there was no match found during scanning; spoofing an infected datagram with a valid datagram; and assembling datagrams into TCP segments.

As per Issue #4, the examiner has shown that Maher did disclose receiving copies of datagrams; reassembling one or more packets into network protocol packets; a reassembled packet queue; a plurality of protocol specific modules; and that only IP packets were reassembled.

As per Issue #5, Issue #6, and Issue #7, the examiner pointed out that there were no new arguments presented and as such the examiner did not comment regarding these issues.

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

Matthew Henning

June 1, 2006

Conferees:

Kim Vu

Christopher Revak

CHRISTOPHER REVAK
PRIMARY EXAMINER

Zilka-Kotab, PC
P.O. BOX 721120
SAN JOSE CA 95172-1120